Elliptic Curves. Sheet 7. To be handed in during 8th Week.

1. Find the ranks of the following elliptic curves.
(a). $Y^2 = X(X^2 + 2X + 3)$.
(b). $Y^2 = X(X^2 + 14X + 1)$.

2. Let $A, +$ be an Abelian group. Let $h : A \to \mathbb{R}_{\geqslant 0}$ satisfy:
(I) There exists a constant C, independent of P, Q, such that
$|h(P + Q) + h(P - Q) - 2h(P) - 2h(Q)| \leqslant C$, for all $P, Q \in A$,
(II) For any $B \in \mathbb{R}$, the set $\{P \in A : h(P) \leqslant B\}$ is finite.
Show that h is a height function on A. Show also that there exists a constant C_3, independent of P, such that $|h(3P) - 9h(P)| \leqslant C_3$, for all $P \in A$.
[$\mathbb{R}_{\geqslant 0}$ denotes $\{x \in \mathbb{R} : x \geqslant 0\}$].

3. A four-letter word $L_1L_2L_3L_4$ has been divided into two pairs: L_1L_2 and L_3L_4. Each of these pairs has been converted into an integer (of at most 4 digits) via the standard map: $A \mapsto 01, B \mapsto 02, \ldots, Z \mapsto 26$. These integers have been encoded by taking each to the power of $d = 4085$, modulo $N = 10481$. The encoded message reads:

$$6012, 3236.$$

You may assume that N is the product of two primes. You should show, in your calculations, how you are only using numbers of length at most 9 digits.
(a) Find a proper factor of N (that is, a factor d of N satisfying $1 < d < N$) by applying Pollard's "$p - 1$" method, using base 2 and exponent 46.
(b) Factorise N by applying the Elliptic Curve Method, using the curve $\mathcal{E} : Y^2 = X^3 - X + 1$ and $3P$, where $P = (5, 11)$.
(c) Use the factorisation of N to decode the message (which is the name of the town famous for being the country music capital of New Zealand).

A Few Pieces of Computational Advice

If you want to perform something like: 2046 · 8018 mod 8777 on a pocket calculator, then the fast way is as follows. First, 2046 · 8018 = 16404828. Now divide by 8777 to get the decimal 1869.070069; now subtract off the integer part 1869 to get .070069; now multiply by 8777 to get the decimal 614.99561; this is guaranteed to be almost exactly an integer, and the nearest integer (namely: 615) will be 16404828 mod 8777. If you want to check it be 100% sure, then you can verify it by: (2046 · 8018 - 615)/8777 and seeing that the result is an exact integer. [N.B. This is much faster than, for example, repeatedly subtracting 8777 from 16404828 until getting a number less than 8777; in this case that approach would require 1869 subtractions!]. This same idea can also make quicker steps of Euclid's Algorithm.

If you want to write a number, such as k=25920, in base 2, then a fast way is as follows. Type 25920 into the calculator. At each step, we reduce the size of our current number either by the step [divide-by-2] (if our current number is even) or by the step [subtract-1-and-then-divide-by-2] (if our current number is odd). This allows us to write down the base 2 digits from right to left, where we write down a 0 if we've done the first of the above, and a 1 if we've done the second. For example, with k=25920, we first perform [divide-by-2] and write down 0 as our rightmost digit (and the calculator display now reads 12960). After doing the [divide-by-2] 5 more times, we have now written a total of 000000 as the six rightmost digits, and the calculator reads: 405. Now, perform [subtract-1-and-then-divide-by-2], and write down a 1 on the left, so that your piece of paper currently reads: 1000000, and your calculator display reads: 202. Now perform [divide-by-2], so that you piece of paper reads: 01000000 and your calculator reads: 101. Continuing until your calculator reads 0 will make your final piece of paper read: 110010101000000; that is: k = $2^6 + 2^8 + 2^{10} + 2^{13} + 2^{14}$ [take care to remember that the last digit in 110010101000000 is the coefficient of 2^0.]